



18.9.2013

valtiovarainministerio@vm.fi

(Viite: Lausuntopyyntö VM008:00/2013)

VÄESTÖREKISTERIKESKUKSEN LAUSUNTO KANSALLISEN PALVELUVÄYLÄN VIITEARKKITEHTUURISTA SEKÄ SEN ALUSTAVASTA TOTEUTUSSUUNNITELMASTA

Väestörekisterikeskus (VRK) toteaa seuraavat huomiot tutustuttuaan Kansallisen palveluväylän viitearkkitehtuuriin ja alustavaan toteuttamissuunnitelmaan:

Kansallisen palveluväylän toteutukselle on asetettu erittäin suuret ja haasteelliset tavoitteet ja koska ratkaisun ennakkoesittely on ollut varsin laajaa, ovat myös odotukset Palveluväylän tuottamalle uudelle toimintatavalle suuret. Riippumatta siitä, millä aikataululla ja ratkaisulla Palveluväylän toteutuksessa tullaan etenemään, VRK on valmis tukemaan hankkeen tavoitteiden toteutumista tarjoamalla viraston tuottamia palveluita Palveluväylän tarpeisiin.

Väestörekisterikeskus on mielellään mukana hankkeessa:

- tarjoamassa kokonaisvaltaisia tunnistusratkaisuja
- tuottamalla väestötietojärjestelmän tiedot palveluväylään
- toteuttamalla varmennetun aikaleimapalvelun palveluväylään
- ja mikäli on tarpeen, olemme valmiita tukemaan hankkeen edistämistä myös muilla tavoin

VRK:lla on valmiudet tuottaa palveluväylän tunnistus- ja allekirjoitusratkaisujen edellyttämät varmennepalvelut kuten sanomaliikenteen asiakas- ja palveluntarjoajan varmennepohjaiseen TLS salaukseen ja viestien allekirjoittamiseen tarvittavat palvelin- ja asiakasvarmenteet sekä loppukäyttäjien tunnistamisessa ja allekirjoittamisessa tarvittavat henkilö- ja ammattilaisvarmenteet. Voimme myös toteuttaa tarvittaessa nopeallakin aikataululla Mittatekniikan keskuksen aikapalveluihin perustuvat varmennetut aikapalvelut, mikäli ne nähdään Palveluväylän toteutuksen kannalta tarpeellisiksi. VRK:lla on olemassa olevat varmennepalvelut palveluvarmenteiden myöntämiseen, tuottamiseen ja varmenteiden elinkaaren hallintaan lukuun ottamatta toteutussuunnitelmassa mainittua koneellista rajapintaa varmenteiden automaattiseen luontiin, välittämiseen ja käyttöönottoon.

VTJ:n palveluiden osalta VRK:lla on valmiudet tuottaa VTJ:n sanomamuotoista tietopalvelua Palveluväylään Pera määrittelyiden mukaisena toteutuksena. Olemme pilotoineet Pera määrittelyjä VTJ:n nykyisissä rajapinnoissa yhdessä VIP:n kanssa, jonka tulosten pohjalta määrittelyt on implementoitavissa VTJ:n tuotantorajapintoihin varsin pienellä kehittämispanoksella. Palveluväylän toteuttamissuunnitelmaan kirjatuista riskeistä:



18.9.2013

Riski: *"Palveluväylän toteuttamiseen varattu aika on liian lyhyt ja toteutusta ei saada tehtyä kyseisessä aikataulussa"*

Alustavassa toteuttamissuunnitelmassa esitetty vaihtoehtoinen toteutusaikataulu on näkemyksemme mukaan realistisempi. Vaikka Palveluväylän toteutuksen pohjana voidaan käyttää xROAD lähdekoodia, tulee järjestelmän sovittaminen kansallisiin ratkaisuihimme olemaan todella iso ja aikaa vaativa ponnistus.

Riski: *"Toteutukseen valitaan vääriä teknologioita. Toteutusta joudutaan myöhemmässä vaiheessa muuttamaan."*

Viitearkkitehtuurissa esitetty palveluväylän tietojen välittämismalli on huomattavasti monimutkaisempi ottaa käyttöön kuin suorat rajapintayhteydet standardin mukaisiin SOAP ja REST rajapintoihin, joihin liittyminen onnistuu nykyaikaisilla sovelluskehittimillä käytännössä napin painalluksella, mikäli tietoliikenneyhteys rajapintaan on auki ja käyttöoikeudet on määritetty. Rajapintatoteutuksissa on tärkeä pyrkiä siihen, että järjestelmän rajapinnat perustuvat mahdollisimman yleisesti käytössä oleviin perusratkaisuihin, jotka ovat yhteensopivia eri elinkaaren vaiheissa olevien asiakasjärjestelmien kanssa ja jotka eivät edellytä asiakasorganisaatioilta merkittäviä hankintoja esim. liityntäpalvelinten toteuttamiseen ja ylläpitoon.

Riski: *"Palveluväylän rahoitus-/liiketoimintamalli ei houkuttele toimijoita palveluväylän käyttäjiksi, palveluväylän käyttö jää vähäiseksi."*

Vaikka Palveluväylä tulee pohjimmiltaan perustumaan Viron xRoad järjestelmän avoimeen lähdekoodiin, tulee Palveluväylän teknisestä infrastruktuurista ja sen ylläpitämiseksi tarvittavista henkilöresursseista merkittäviä jatkuvia kustannuksia. Palveluväylän rahoitusmalli ei saisi olla ristiriidassa julkishallinnon tietopalveluiden maksuttomuuden tavoitteiden kanssa, jota julkishallinnon tietoja hyödyntävät palveluntuottajat ovat peräänkuuluttaneet koko 2000 luvun ajan, ja mihin suuntaan on nyt vihdoinkin oltu asteittain siirtymässä.

Muut huomiot:

Lausuntokierroksella ollut aineisto ei sisällä Palveluväylän viitearkkitehtuurissa viitattua kustannus-hyötyarviota, jonka laadinta ja arviointi olisi ehdottoman tärkeää tehdä ennen kuin näin mittavaa kehityshanketta aletaan viedä eteenpäin. Koska kansallisten perusrekisteriemme rajapintapalvelut edustavat jo nykyisellään kansainvälistä kärkeä ja niiden tekninen käyttöönotto on jo nykyisellään asiakasjärjestelmien kannalta helppoa, on Palveluväylällä aikaansaattava kustannushyöty vaikea hahmottaa. Palveluväylän viitearkkitehtuurissa esitellyn ratkaisun rinnakkaisena vaihtoehtona voisi arvioida, saisimmeko mahdollisesti pienemmin kehittämisponnistuksin kuten asiakasprosessien sähköistämisen ja virtaviivaistamisen avulla Palveluväylän aikaan jo nykyisillä tietovarantokohtaisilla rajapinnoilla ja palveluprosesseilla yhdistämällä kokonaisuuteen esim. lupapalveluiden koontia yhteen portaaliin. Samalla Palveluväylän toteutuksessa voitaisiin keskittyä paremmin Suomessa jo vuosia avoimena olleeseen kansallisen tunnistusratkaisun aikaansaamiseen.

Palveluväylän toteutuksessa olisi syytä ottaa huomioon EU:n komissiosta jo piakkoin asetuksena voimaan tuleva luottamuspalveluiden sääntely, joka säätelee tunnistamisen palveluista yleiseurooppalaisella tasolla. Erityisesti yritysten allekirjoitusvarmenteiden ja aikaleimaan liittyvät kysymykset olisi hyvä ratkaista kansallisesti palveluväylän toteuttamisen yhteydessä. Asetusehdotus ottaa kantaa myös hyväksyttävien kansallisten identiteettien tasovaatimuksiin.

18.9.2013

Palveluväylän viitearkkitehtuurissa esitetään, että palveluväylän lokipalvelun kiistämättömyys toteutettaisiin pohjautuen md5- tiivisteisiin tai muuhun luotettavasti toteutettuun tiivisteeseen. Koska md5 tiivistefunktiot on jo vuosia sitten todettu turvattomaksi, olisi lokitiedot järkevää varmentaa SHA1 tai mieluiten SHA256 tiivistein.

Palveluväylässä toteutettava aikapalvelu olisi järkevää tuottaa varmennettuna aikapalveluna, jotta tapahtumien ajankohta olisi todennettavissa kiistämättömästi.

Ylijohtaja



Hannu Luntiala

Johtaja



Lea Krohns

